

Tillståndsmyndigheten för användning  
av social- och hälsovårdsdata

datum 5.10.2020

Föreskriften har utfärdats	5.10.2020
Föreskriften träder i kraft	1.5.2021
Gäller	Tills vidare
Rättslig grund	Lag om sekundär användning av personuppgifter inom social- och hälsovården (552/2019) 22 § 3 mom. samt 24 § 2 mom. (nedan ”lagen om sekundär användning”)

## **Föreskrift av Tillståndsmyndigheten för användning av social- och hälsovårdsdata: Krav som ska ställas på andra tjänsteleverantörers informationssäkra driftmiljöer**

### **1 Bakgrund**

Tillståndsmyndigheten för användning av social- och hälsovårdsdata Findata (nedan ”Tillståndsmyndigheten”) förvaltar en informationssäker driftmiljö i enlighet med 20 § 1 mom. i lagen om sekundär användning. De datamaterial för vilka Tillståndsmyndigheten har beviljat användningstillstånd lämnas i regel ut för behandling av tillståndshavaren i denna driftmiljö.

Om ansökan om dataanvändningstillstånd innehåller en begäran om att datamaterial ska lämnas ut för behandling i en annan miljö än Tillståndsmyndighetens informationssäkra driftmiljö, ska det enligt 20 § 3 mom. i lagen om sekundär användning i ansökan särskilt motiveras varför detta är nödvändigt. Tillståndsmyndigheten eller någon annan myndighet som avses i lagen om sekundär användning får då lämna ut uppgifter till sökanden endast om driftmiljön uppfyller villkoren i 20 § 2 mom. och i 21–29 § i denna lag.

Om en enskild personuppgiftsansvarig som avses i 44 § 3 mom. i lagen om sekundär användning har fattat ett beslut om dataanvändningstillstånd för uppgifter som ingår i de egna registren, ska den personuppgiftsansvariga alltid lämna ut datamaterialet till tillståndshavaren för behandling i en informationssäker driftmiljö som avses i 20 § i lagen om sekundär användning.

Enligt 24 § 2 mom. i lagen om sekundär användning meddelar Tillståndsmyndigheten närmare föreskrifter om de krav som ska ställas på andra tjänsteleverantörers informationssäkra driftmiljöer. Kraven ska förutsätta informationssäkerhet på motsvarande nivå som i Tillståndsmyndighetens egen driftmiljö.

Innan föreskriften trädde i kraft var den ute på remiss 22.5–26.6.2020, och sammanlagt 54 utlåtanden gavs under denna period. Utlåtandena har beaktats i beredningen av föreskriften.

Kraven på informationssäkra driftmiljöer finns i bilaga 1 till denna föreskrift.

Tillståndsmyndigheten för användning  
av social- och hälsovårdsdata

datum 5.10.2020

## 2 Föreskriftens tillämpningsområde

Denna föreskrift är en i 24 § 2 mom. i lagen om sekundär användning avsedd föreskrift av Tillståndsmyndigheten om krav som ska ställas på andra tjänsteleverantörers informationssäkra driftmiljöer.

Denna föreskrift tillämpas på alla de användningsändamål som föreskrivs i lagen om sekundär användning för vilka det enligt denna lag behövs dataanvändningstillstånd. Dessa användningsändamål är vetenskaplig forskning, statistikföring, undervisning samt myndigheternas planerings- och utredningsuppgifter. I fråga om undervisningen gäller föreskriften framställning av undervisningsmaterial, inte den egentliga undervisningen.

Uppfyllande av kraven i denna föreskrift är en förutsättning för att Tillståndsmyndigheten ska kunna pröva och lämna ut datamaterial för behandling av tillståndshavaren i en annan miljö än tillståndsmyndighetens egen från och med den 1 maj 2021.

Uppfyllandet av kraven i denna föreskrift verifieras med ett intyg som utfärdats av ett bedömningsorgan för informationssäkerhet. Bestämmelser om bedömning av informationssäkerhet finns i 26 § i lagen om sekundär användning.

## 3 Föreskriftens giltighetstid och ändringar

Denna föreskrift gäller tills vidare.

## 4 Tillämpade rättsnormer

Lagen om sekundär användning av personuppgifter inom social- och hälsovården (552/2019) 18–34 §, 60 § 1 mom.

Johanna Seppänen  
Direktör

Heikki Lanu  
IKT-chef

Denna föreskrift har undertecknats elektroniskt.

## Bilaga 1: Krav på informationssäkra driftmiljöer

### Innehåll

<b>1 Allmänt.....</b>	<b>3</b>
1.1 Definitioner.....	3
1.2 Funktionell beskrivning .....	5
1.3 Systemarkitektur.....	6
1.4 Tjänsteleverantörer .....	6
1.5 Betrodda autentiseringskällor.....	7
<b>2 Tekniska krav.....</b>	<b>7</b>
2.1 Identifiering .....	7
2.1.1 Krav enligt lagen om sekundär användning.....	7
2.1.2 Krav som ställs av Tillståndsmyndigheten.....	7
2.2 Hantering av användare och åtkomsträttigheter .....	8
2.2.1 Krav enligt lagen om sekundär användning.....	8
2.2.2 Krav som ställs av Tillståndsmyndigheten.....	8
2.3 Skydd av miljön .....	8
2.3.1 Krav enligt lagen om sekundär användning.....	8
2.3.2 Krav som ställs av Tillståndsmyndigheten.....	8
2.4 Loggning.....	10
2.4.1 Krav enligt lagen om sekundär användning.....	10
2.4.2 Krav som ställs av Tillståndsmyndigheten.....	10
2.5 Hantering och övervakning av miljön.....	10
2.5.1 Krav som ställs av Tillståndsmyndigheten.....	10
2.6 Avlägsnande av material från driftmiljön.....	11
2.6.1 Krav som ställs av Tillståndsmyndigheten.....	11
<b>3 Aktörens tillförlitlighet .....</b>	<b>12</b>
3.1 Allmänt .....	12
3.1.1 Krav enligt lagen om sekundär användning.....	12
3.1.2 Krav som ställs av Tillståndsmyndigheten.....	12
3.2 Dataskydd.....	13
3.2.1 Krav som ställs av Tillståndsmyndigheten.....	13
3.3 Lokaler .....	13
3.3.1 Krav som ställs av Tillståndsmyndigheten.....	13

Tillståndsmyndigheten för användning  
av social- och hälsovårdsdata

Krav på informationssäkra driftmiljöer

3.4 Personal.....	13
3.4.1 Krav som ställs av Tillståndsmyndigheten.....	13
<b>4 Viktiga processfaser i anslutning till en informationssäker driftmiljö.....</b>	<b>14</b>

Tillståndsmyndigheten för användning  
av social- och hälsovårdsdata

Krav på informationssäkra driftmiljöer

## 1 Allmänt

Detta dokument beskriver och preciserar informationssäkerhetskraven för informationssäkra driftmiljöer som förutsätts i lagen om sekundär användning (Lag om sekundär användning av personuppgifter inom social- och hälsovården, 552/2019). En tjänsteleverantör förutsätts iaktaga de allmänna informationssäkerhetskraven i 18 §. Med en informationssäker driftmiljö säkerställs att de uppgifter som lämnats ut med stöd av lagen om sekundär användning hanteras på ett informationssäkert sätt i enlighet med tillståndet. Myndigheten får lämna ut datamaterial till sökanden endast om driftmiljön uppfyller villkoren i 20 § 2 mom. och i 21–29 §.

Syftet med informationssäkerhetskraven är att säkerställa att tjänsteleverantören av en informationssäker driftmiljö har tillräckliga säkerhetsarrangemang för att förhindra att sekretessbelagda uppgifter obehörigen avslöjas. Denna föreskrift tar inte ställning till det tekniska genomförandet och därför måste kraven granskas från fall till fall.

Det bedömningsorgan för informationssäkerhet som utför bedömningen och utfärdar intyget bedömer med hjälp av sin yrkeskunskap om de gällande informationssäkerhetscertifikaten för en informationssäker driftmiljö lämpar sig för att uppfylla kraven i föreskriften. Tillståndsmyndigheten gör ingen bedömning av och erbjuder ingen teknisk rådgivning om informationssäkerheten i en informationssäker driftmiljö.

I informationssäkerhetskraven hänvisas det till följande bestämmelser och kriterier:

- Lag om sekundär användning av personuppgifter inom social- och hälsovården (552/2019)
- KATAKRI 2015 - Verktyg för informationssäkerhetsauditering för myndigheter
  - I tillämpningen ska man beakta KATAKRI-skyddsnivån och/eller punkterna i exemplet, om sådana har presenterats
- PiTuKri version 1.1. mars 2020 – Bedömningskriterier för säkerheten av molntjänster
- Europaparlamentets och rådets förordning (EU) 2016/679 av den 27 april 2016 om skydd för fysiska personer med avseende på behandling av personuppgifter och om det fria flödet av sådana uppgifter och om upphävande av direktiv 95/46/EG (allmän dataskyddsförordning)
- Europaparlamentets och rådets förordning (EU) nr 910/2014 av den 23 juli 2014 om elektronisk identifiering och betrodda tjänster för elektroniska transaktioner på den inre marknaden och om upphävande av direktiv 1999/93/EG
- Standarden ISO/IEC 27001

### 1.1 Definitioner

I denna föreskrift:

- Med material avses datamaterial som innehåller personuppgifter.

Tillståndsmyndigheten för användning  
av social- och hälsovårdsdata

Krav på informationssäkra driftmiljöer

- Med fysiskt och tekniskt skyddat område avses en miljö där lokaler och tekniska lösningar hindrar utomstående från att okontrollerat få tillgång till uppgifterna. Krav på utrymmen beskrivs i punkt 3.3 Lokaler.
- Med karantänmiljö avses en avskild och skyddad lösning där krypterat material omvandlas till klarspråk och en granskning av datasäkerhet och skadliga program utförs. I samma miljö krypteras material som ska skickas till Tillståndsmyndigheten för granskning inför leveransen. Miljön får inte vara ansluten till internet.
- Med användarmiljö avses en databehandlingsmiljö i en informationssäker driftmiljö som är åtskild enligt dataanvändningstillståndet där kunden/forskaren eller -gruppen behandlar material som innehåller personuppgifter. Miljön får inte vara direkt ansluten till internet eller till andra driftmiljöer.
- Med användar- och åtkomsthantering avses en lösning som ligger mellan den egentliga forskningsmiljön och internet och som används för att identifiera användare och för åtkomstkontroll.
- Med logghantering avses en åtskild och skyddad lösning som används för att samla in, övervaka och rapportera logguppgifter i driftmiljön.
- Logguppgifter är bl.a. logguppgifter om användning och utlämnande samt tekniska logguppgifter som samlas in av apparater i driftmiljön.
- Tjänsteleverantören är den aktör som ansvarar för driftmiljön och dess överensstämmelse med kraven och som också kan anlita underleverantörer.
- Hantering av den tekniska, organisatoriska och fysiska informationssäkerheten innebär hanterings- och övervakningslösningar för olika delområden i anslutning till genomförandet av driftmiljön.
- Med Tillståndsmyndighetens system avses informationssystem som administreras av Tillståndsmyndigheten där man bl.a. behandlar tillstånd samt överför, sammanställer, förbehandlar, sammanfogar, pseudonymiserar och anonymiserar material.
- Med en informationssäker driftmiljö (i fortsättningen även enbart driftmiljö) avses en teknisk, organisatorisk och fysisk miljö för behandling av uppgifter.
- Informationssäkerhetskanning innebär att databehandlingsmiljön inspekteras med tekniska hjälpmedel. På detta sätt säkerställer man bl.a. att det inte finns sårbarheter eller felaktiga konfigurationer som äventyrar informationssäkerheten.
- En autentiseringskälla är ett system där de identifieringskoder som identifieringen och behörighetshanteringen kräver finns.
- Principen om minsta möjliga rättigheter är ett it-säkerhetsbegrepp som innebär att åtkomsträttigheter till ett informationssystem ska begränsas till de snävaste möjliga rättigheterna med vilka användaren eller processen kan utföra den uppgift som ålagts den.

Tillståndsmyndigheten för användning  
av social- och hälsovårdsdata

Krav på informationssäkra driftmiljöer

Åtkomsträttigheterna ska också begränsas till den tidsmässigt kortast möjliga tidsperioden under vilken uppgiften kan utföras.

## 1.2 Funktionell beskrivning

Med en informationssäker driftmiljö avses en teknisk, organisatorisk och fysisk driftmiljö för behandling av uppgifter där informationssäkerheten har säkerställts genom lämpliga administrativa och tekniska åtgärder. I en informationssäker driftmiljö ska det vara möjligt att säkerställa en informationssäker behandling av uppgifterna enligt dataanvändningstillståndet och endast de användare som specificeras i dataanvändningstillståndet ges åtkomst till den användarmiljö som inrättas för projektet i fråga.

En tjänsteleverantör är en aktör som tillhandahåller kunderna tjänster som syftar till en informationssäker driftmiljö. Tjänsteleverantören kan vid behov anlita underleverantörer för olika delhelheter, till exempel i fråga om processering och lagringskapacitet. Tjänsteleverantören ansvarar för att en informationssäker driftmiljö och de parter som deltar i produktionen av den uppfyller kraven i denna föreskrift.

De viktigaste funktionaliteterna i anslutning till en informationssäker driftmiljö:

- Man loggar in i användarmiljön med koder från betrodda autentiseringskällor.
- För inloggning i användarmiljön används i regel tvåfaktorsautentisering.
- I användarmiljön får kunden endast tillgång till det material som avses i dataanvändningstillståndet.
- Om kunden har flera dataanvändningstillstånd har han eller hon möjlighet att i användarmiljön behandla material med endast ett dataanvändningstillstånd åt gången.
- Överföringen av personuppgiftsmaterial till en informationssäker driftmiljö sker på ett informationssäkert sätt.
- Det ska inte vara möjligt att skapa direkta internetförbindelser i användarmiljön.
- Behandlingen av identifierbart personuppgiftsmaterial ska kunna skyddas särskilt omsorgsfullt i alla skeden av behandlingen.
- Logghanteringen ska ske i en skyddad miljö där det inte är möjligt att ansluta direkt till internet.

Arkitekturen för en informationssäker driftmiljö beskrivs nedan och de viktigaste processfaserna som gäller tjänsteleverantören beskrivs i punkt 4.

### 1.3 Systemarkitektur

Bilden nedan beskriver den grundläggande systemarkitekturen för en informationssäker driftmiljö. Syftet är att klargöra vilka funktioner en informationssäker driftmiljö består av och hur den anknyter till andra centrala funktioner enligt lagen om sekundär användning.

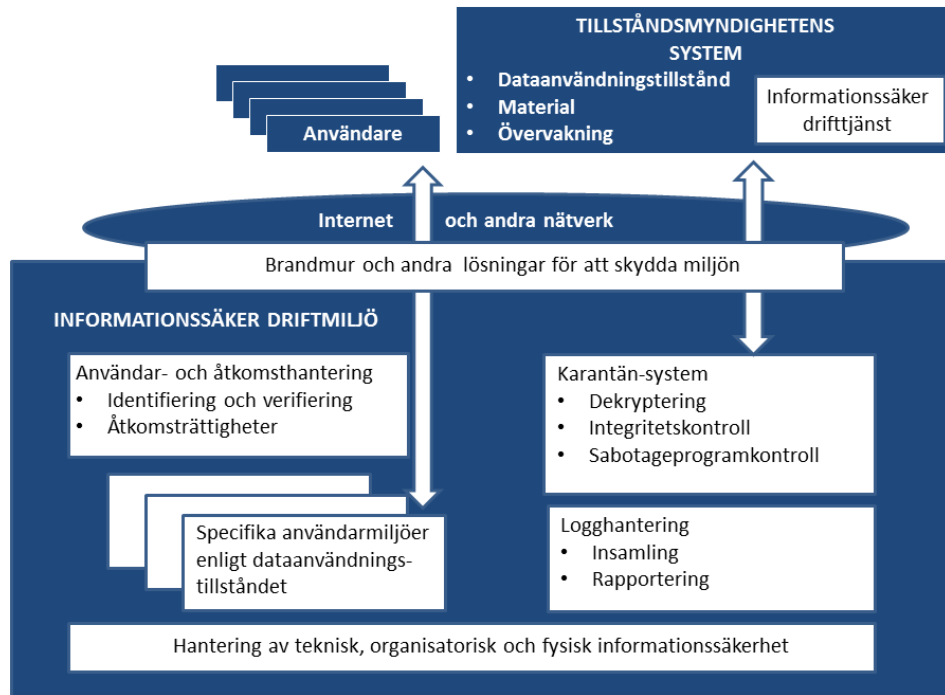


Bild: Grundläggande systemarkitektur för en informationssäker driftmiljö

### 1.4 Tjänsteleverantörer

En informationssäker driftmiljö ska ha en namngiven tjänsteleverantör som ansvarar för att kraven i denna föreskrift uppfylls. Tjänsteleverantören kan anlita underleverantörer till exempel för att producera informationstekniska tjänster, men tjänsteleverantören ansvarar alltid för att en informationssäker driftmiljö överensstämmer med kraven. I praktiken måste det finnas ett bindande avtalsförhållande mellan tjänsteleverantören och underleverantören.

Tjänsteleverantören ska också identifiera en eventuell kumulativ effekt av personuppgifterna och beakta detta i skyddet av den driftmiljö som tjänsteleverantören tillhandahåller. Kumulativa effekter kan uppstå till exempel i situationer där avsikten är att lagra flera personuppgiftsmaterial i driftmiljön och/eller materialets storlek blir stor. Tillstånds- och tillsynsverket för social- och hälsovården Valvira för ett offentligt register över driftmiljöer som uppfyller kraven och anmälts till verket.



Tillståndsmyndigheten för användning  
av social- och hälsovårdsdata

Krav på informationssäkra driftmiljöer

## 1.5 Betrodda autentiseringskällor

Tillståndsmyndigheten upprätthåller en uppdaterad lista över betrodda autentiseringskällor och publicerar dem på adressen [www.findata.fi](http://www.findata.fi). Tjänsteleverantören kan också skapa en autentiseringskälla i anslutning till sin informationssäkra driftmiljö. Källan kan anses vara tillförlitlig om den uppfyller kraven i denna föreskrift.

## 2 Tekniska krav

### 2.1 Identifiering

#### 2.1.1 Krav enligt lagen om sekundär användning

21 § Identifiering av användare i informationssäkra driftmiljöer  
<https://finlex.fi/sv/laki/ajantasa/2019/20190552#L3P21>

#### 2.1.2 Krav som ställs av Tillståndsmyndigheten

1. Den första identifieringen av användaren görs i första hand med stark autentisering, till exempel med Suomi.fi-tjänsten. Om det inte är möjligt att göra den första identifieringen med stark autentisering, ska användarens identitet verifieras med identitetshandlingar i användarens närvaro på ett dokumenterat sätt. Om det t.ex. på grund av resor inte är rimligt att kräva att användaren ska närvara, kan den första identifieringen genomföras på ett sätt där en organisation som står i ett arbets-, uppdrags-, avtals- eller motsvarande förhållande till användaren bekräftar användarens identitet skriftligen och bindande med nödvändiga dokument.
2. Mellan innehavarna av koderna och autentiseringskällan ska det antingen finnas ett avtalsförhållande (till exempel ett arbets- eller forskningsavtal), en affiliation (till exempel via ett forskningsprojekt) eller ett annat juridiskt bindande förhållande. Administratörer av autentiseringskällor är skyldiga att stänga av koder omedelbart efter att avtalsförhållandet upphört eller om de misstänker att koderna läckt ut eller på annat sätt missbrukas.
3. Identifieringen ska ske med tvåfaktorsautentisering där minst två olika identifieringsmetoder används. Utöver kombinationen av användarnamn och lösenord används en separat identifierare, till exempel en mobilapplikation eller någon annan motsvarande identifieringsmetod. Tvåfaktorsautentiseringen ska ha skett innan användaren börjar behandla material enligt dataanvändningstillståndet.
4. Om en terminal som är dedikerad för användning i användarmiljön och som tjänsteleverantören ordnat och allokerat för användaren finns inom samma fysiskt och tekniskt skyddade område som användarmiljön, krävs ingen tvåfaktorsautentisering, men användarens identitet ska ha verifierats innan den dedikerade terminalen överläts för användning.
5. Förutom punkterna ovan ska KATAKRI-punkterna I 06 (punkterna 1–10 i exemplet) och I 07 (punkterna 1–7 i exemplet) tillämpas.

Tillståndsmyndigheten för användning  
av social- och hälsovårdsdata

Krav på informationssäkra driftmiljöer

## 2.2 Hantering av användare och åtkomsträttigheter

### 2.2.1 Krav enligt lagen om sekundär användning

22 § Åtkomsträttigheter för användare i informationssäkra driftmiljöer  
<https://finlex.fi/sv/laki/ajantasa/2019/20190552#L3P22>

### 2.2.2 Krav som ställs av Tillståndsmyndigheten

1. Åtkomsträttigheterna till miljön är begränsade så att användarna endast får tillgång till de material och resurser för vilka de har beviljats tillstånd.
2. Åtkomsträttigheterna till miljön är begränsade enligt dataanvändningstillståndet. Om en person har flera dataanvändningstillstånd i miljön får han eller hon endast tillgång till ett dataanvändningstillstånd åt gången.
3. Åtkomsträttigheter till miljön beviljas enligt principen om minsta möjliga rättigheter (KATAKRI I 02).
4. I miljön används endast koder från betrodda identifieringskällor.
5. Vid upptäckt av missbruk ska tjänsteleverantören utan dröjsmål förhindra ytterligare skador till exempel genom att begränsa åtkomsträttigheterna.
6. Åtkomsträtten till användarmiljön låses automatiskt efter att dataanvändningstillståndet har upphört att gälla.
7. Materialet i användarmiljön avlägsnas automatiskt senast efter sex månader efter att åtkomsträtten upphört, om inte annat bestäms i lagen.
8. Förutom punkterna ovan ska punkt I 06 (punkterna 1–10 i exemplet) i KATAKRI tillämpas.

## 2.3 Skydd av miljön

### 2.3.1 Krav enligt lagen om sekundär användning

18 § Allmänna informationssäkerhetskrav <https://finlex.fi/sv/laki/ajantasa/2019/20190552#L3P18>

23 § Skydd för informationssäkra driftmiljöer <https://finlex.fi/sv/laki/ajantasa/2019/20190552#L3P23>

24 § Minimikrav på informationssäkra driftmiljöer  
<https://finlex.fi/sv/laki/ajantasa/2019/20190552#L3P24>

### 2.3.2 Krav som ställs av Tillståndsmyndigheten

1. Åtkomsthanteringsmiljön ska skyddas enligt KATAKRI I 01 Skyddsnivå IV.

Tillståndsmyndigheten för användning  
av social- och hälsovårdsdata

Krav på informationssäkra driftmiljöer

2. I fråga om användarmiljön och karantänmiljön ska skyddet ske enligt KATAKRI I 01 Skyddsnivå IV.
3. Preciseringar av kraven:
  - a. Användarmiljön är åtskild från internet med en brandväggslösning.
  - b. Om en terminal som är dedikerad för användning i användarmiljön och som tjänsteleverantören allokerat för användaren finns inom samma fysiskt och tekniskt skyddade område som användarmiljön, krävs ingen tvåfaktorsautentisering, men användarens identitet ska ha verifierats innan den dedikerade terminalen överläts för användning. Terminalen får inte vara ansluten till ett nätverk utanför användarmiljön och användaren får inte ha möjlighet att importera eller exportera uppgifter från användarmiljön med hjälp av terminalen, t.ex. med hjälp av ett USB-minne.
  - c. Om terminalen inte är belägen inom samma fysiskt och tekniskt skyddade område som användarmiljön, ska inloggningen göras med en tvåfaktorsautentisering där det andra steget ska genomföras innan åtkomst till materialet medges.
  - d. Direkta förbindelser från användarens terminal till användarmiljön tillåts inte. Via förbindelse överförs till exempel endast skärmbilden samt inmatningar från tangentbord och mus.
  - e. Användarmiljöerna för olika dataanvändningstillstånd ska vara åtskilda så att endast de användare som nämns i dataanvändningstillståndet i fråga får tillgång till informationsmaterialet som tillståndet avser.
  - f. Användarna beviljas inte underhållsrättigheter till datorer i driftmiljön. Här tillämpas KATAKRI I 06 (punkterna 1–10 i exemplet) och iakttas principen om minsta möjliga rättigheter.
  - g. När det gäller nätslusslösningar mellan miljöer på olika skyddsnivåer tillämpas punkterna 1–3 i exemplet i KATAKRI I 01.
4. I skyddet av systemet tillämpas principen om minimifunktioner och minsta möjliga rättigheter enligt KATAKRI I 08 (punkterna 1–17 i exemplet).
5. I skyddet av systemet tillämpas principen om skydd på flera nivåer enligt KATAKRI I 09, I 13 (punkterna 1–3 i exemplet).
6. Om den personuppgiftsansvarige behöver överföra tillståndspliktigt material i sin egen miljö till en egen informationssäker driftmiljö inom samma fysiskt och tekniskt skyddade område, kan överföringen också utföras utan en informationssäker drifttjänst. Här tillämpas punkt I 15 (Exempel 2) i KATAKRI på lämpligt sätt.
7. I hanteringen av sårbarheter i programvara ska punkt I 23 (punkterna 1–2 i exemplet) i KATAKRI tillämpas.

Tillståndsmyndigheten för användning  
av social- och hälsovårdsdata

Krav på informationssäkra driftmiljöer

8. Regelbundna informationssäkerhetskontroller av driftmiljön ska utföras.

## 2.4 Loggning

### 2.4.1 Krav enligt lagen om sekundär användning

19 § Logguppgifter <https://finlex.fi/sv/laki/ajantasa/2019/20190552#L3P19>

### 2.4.2 Krav som ställs av Tillståndsmyndigheten

1. Logguppgifter ska behandlas på samma informationssäkra sätt som personuppgifter som hör till särskilda personuppgiftskategorier.
2. I användningsloggarna ska uppgifter sparas om den personuppgiftsansvarige, användningsändamålet enligt lagen om sekundär användning, det dataanvändningstillstånd som berättigar till behandling, den användare som har rätt att behandla uppgifterna enligt dataanvändningstillståndet, uppgifter och uppgiftsgrupper som behandlas samt användningstidpunkten.
3. Tekniska logguppgifter ska samlas in på ett heltäckande sätt för att eventuella felfunktioner eller dataintrång ska kunna utredas tillräckligt heltäckande. Dessa tekniska loggar ska förvaras i minst fem år.
4. I övrigt i loggningen tillämpas anvisningarna i KATAKRI I 10 (punkterna 1–7 i exemplet).
5. Administrationsförbindelserna och användningen ska skyddas enligt KATAKRI I 04.
6. Loggarna ska följas upp och analyseras systematiskt och regelbundet.
7. Insamlingen av logguppgifter ska vara utförd på ett sådant sätt att logguppgifter sparas i systemet även då användaren enbart sett personuppgifter.
8. Tillståndsspecifika logguppgifter om materialanvändning och användarregister ska på Tillståndsmyndighetens begäran lämnas in utan obefogat dröjsmål.

## 2.5 Hantering och övervakning av miljön

### 2.5.1 Krav som ställs av Tillståndsmyndigheten

1. Driftmiljön är dokumenterad och dokumenteringen ska kunna användas vid bedömningsorganets bedömning samt vid andra inspektioner.
2. Driftmiljön ska övervakas automatiskt dygnet runt.
3. Vid övervakningen av driftmiljön ska särskild uppmärksamhet fästas vid övervakningen av informationssäkerheten.

Tillståndsmyndigheten för användning  
av social- och hälsovårdsdata

Krav på informationssäkra driftmiljöer

4. Vid observation av avvikelser i driftmiljön ska kriterierna i KATAKRI I 11 användas i tillämpliga delar.
5. Det ska regelbundet övervakas och granskas att driftmiljöns informationssäkerhet är uppdaterad.
6. Hanteringen av driftmiljön ska göras från en i fråga om informationssäkerheten åtstramad arbetsstation via en krypterad datakommunikationsförbindelse.
7. Driftmiljön ska underhållas i lämpliga lokaler.
8. Driftmiljöns servrar ska vara placerade i skyddade lokaler enligt anvisningarna i KATAKRI F 01.
9. Underhållsrättigheterna för driftmiljön ska vara personliga åtkomsträttigheter som definieras separat enligt arbetsuppgifterna.
10. Underhållsrättigheterna för driftmiljön ska vid behov delas in i underhållsrättigheter på olika nivåer (Administration Tier Model).
11. I underhållsrättigheterna för driftmiljön tillämpas principen om minsta möjliga rättigheter enligt KATAKRI I 06 (punkterna 1–10 i exemplet) samt principen om skydd på flera nivåer enligt KATAKRI I 07 (punkterna 1–7 i exemplet).
12. I hanteringen och övervakningen av driftmiljön iaktas sektionerna I 03 och I 04 i KATAKRI i tillämpliga delar.
13. I hanteringen av ändringar i driftmiljön tillämpas sektion I 20 i KATAKRI (punkterna 1–3 i exemplet) i tillämpliga delar.
14. Även de åtgärder som vidtas av dem som upprätthåller den informationssäkra driftmiljön ska inkluderas i logghanteringen.
15. Om man misstänker att behandlingen av uppgifterna strider mot lagen eller villkoren i dataanvändningstillståndet, ska tjänsteleverantören utan dröjsmål kunna anmäla saken till Tillståndsmyndigheten och lämna en detaljerad utredning om saken. Detta utesluter inte andra skyldigheter enligt lagstiftningen.

## 2.6 Avlägsnande av material från driftmiljön

### 2.6.1 Krav som ställs av Tillståndsmyndigheten

1. Materialet ska avlägsnas från driftmiljön sex månader efter att dataanvändningstillståndet har upphört gälla, om inget annat följer av dataanvändningstillståndet.
2. Vid avlägsnande av materialet tillämpas anvisningarna i KATAKRI I 19 (punkterna 2 och 3 i exemplet).

Tillståndsmyndigheten för användning  
av social- och hälsovårdsdata

Krav på informationssäkra driftmiljöer

3. Vid förvaringen av materialet ska eventuella villkor i dataanvändningstillståndet beaktas.

## 3 Aktörens tillförlitlighet

### 3.1 Allmänt

#### 3.1.1 Krav enligt lagen om sekundär användning

20 § Informationssäker driftmiljö <https://finlex.fi/sv/laki/ajantasa/2019/20190552#L3P20>

25 § Påvisande av informationssäkerhet i en informationssäker driftmiljö  
<https://finlex.fi/sv/laki/ajantasa/2019/20190552#L3P25>

26 § Bedömning av informationssäkerhet <https://finlex.fi/sv/laki/ajantasa/2019/20190552#L3P26>

27 § Återkallande av bedömningsorganets intyg  
<https://finlex.fi/sv/laki/ajantasa/2019/20190552#L3P27>

28 § Anmälningsskyldighet för bedömningsorgan för informationssäkerhet  
<https://finlex.fi/sv/laki/ajantasa/2019/20190552#L3P28>

29 § Uppföljning efter ibrukttagande av informationssäker driftmiljö  
<https://finlex.fi/sv/laki/ajantasa/2019/20190552#L3P29>

30 § Övervakning och inspektioner av informationssystem  
<https://finlex.fi/sv/laki/ajantasa/2019/20190552#L3P30>

31 § Rätt för Tillstånds- och tillsynsverket för social- och hälsovården att anlita utomstående experter  
<https://finlex.fi/sv/laki/ajantasa/2019/20190552#L3P31>

32 § Rätt för Tillstånds- och tillsynsverket för social- och hälsovården att få information  
<https://finlex.fi/sv/laki/ajantasa/2019/20190552#L3P32>

33 § Tillstånds- och tillsynsverket för social- och hälsovårdens åläggande att avhjälpa brister samt vite  
<https://finlex.fi/sv/laki/ajantasa/2019/20190552#L3P33>

34 § Föreläggande att fullgöra skyldigheter <https://finlex.fi/sv/laki/ajantasa/2019/20190552#L3P34>

#### 3.1.2 Krav som ställs av Tillståndsmyndigheten

1. En informationssäker driftmiljö ska fysiskt vara belägen inom EU/EES-området.
2. Tjänsteleverantören av en informationssäker driftmiljö ska vara en organisation som är registrerad inom EU/EES-området.
3. Tjänsteleverantörens tillförlitlighet ska kunna bedömas med tillämpning av PiTuKri kapitel ”Produktion av tjänsten” (s. 12).

Tillståndsmyndigheten för användning  
av social- och hälsovårdsdata

Krav på informationssäkra driftmiljöer

4. Tjänsteleverantören ska påvisa tillförlitligheten med ett säkerhetshanteringssystem, till exempel enligt standarden ISO/IEC 27001.
5. Tillstånds- och tillsynsverket för social- och hälsovården (Valvira) eller en utomstående sakkunnig som verket anvisar har rätt att utföra inspektioner som krävs för tillsynen. För att utföra en inspektion har en inspektör rätt att få tillträde till alla lokaler där det bedrivs verksamhet som avses i denna lag eller där det förvaras uppgifter som är viktiga för tillsynen över efterlevnaden av denna lag. Kravet gäller även de underleverantörer som tjänsteleverantören använder.

## 3.2 Dataskydd

### 3.2.1 Krav som ställs av Tillståndsmyndigheten

1. En konsekvensbedömning avseende dataskydd (DPIA) enligt artikel 35 i EU:s allmänna dataskyddsförordning (GDPR) ska göras av driftmiljön.
2. De skyldigheter och avtal som gäller den personuppgiftsansvarige och personuppgiftsbiträdet har beaktats i enlighet med de gällande anvisningarna i dataskyddsförordningen. Förordningen innehåller inga anvisningar utan är direkt förpliktande.
3. Tjänsteleverantören ansvarar för att de program, koder eller dylikt som överförs till och används i driftmiljön och användarmiljön inte äventyrar informationssäkerheten vid behandling av personuppgifter. Det är särskilt viktigt att säkerställa att personuppgifter inte flyttas ut ur användarmiljön på annat sätt än vad som föreskrivs om överföring av material.

## 3.3 Lokaler

### 3.3.1 Krav som ställs av Tillståndsmyndigheten

1. Underhållet av miljön ska ske i lokaler som godkänts av bedömningsorganet för informationssäkerhet.
2. Underhållet av servrar ska ske i lokaler som godkänts av bedömningsorganet för informationssäkerhet.
3. När det gäller lokalsäkerhet iakttas KATAKRI:s bedömningskriterier för fysisk säkerhet F 01–08 i tillämpliga delar.

## 3.4 Personal

### 3.4.1 Krav som ställs av Tillståndsmyndigheten

Personer som arbetar med underhåll av driftmiljön och som har tillgång till personuppgiftsmaterial ska ha genomgått en normal säkerhetsutredning eller någon annan motsvarande myndighetsutredning.

Tillståndsmyndigheten för användning  
av social- och hälsovårdsdata

Krav på informationssäkra driftmiljöer

1. Personal som har tillgång till personuppgiftsmaterial ska vara förtrogen med anvisningarna för behandlingen av materialet.
2. I fråga om personalsäkerhet tillämpas KATAKRI T 08–12.

#### 4 Viktiga processfaser i anslutning till en informationssäker driftmiljö

Processfas	Uppgifter	Observera
Säkerställande av överensstämmelse med kraven	Tjänsteleverantören ska se till att ha ett giltigt intyg över informationssäkerheten i driftmiljön som utfärdats av ett bedömningsorgan för informationssäkerhet.	(Jfr 552/2019 25 §) Intyget ska omfatta alla delområden i den informationssäkra driftmiljön där personuppgifter behandlas och delområden som påverkar genomförandet av personuppgifternas dataskydd.
	Tillståndsmyndigheten kontrollerar i Tillstånds- och tillsynsverket för social- och hälsovårdens offentliga register att tjänsteleverantören har ett giltigt intyg.	(Jfr 552/2019 28 §, 30 §)
	Tjänsteleverantören ger tillsynsmyndigheten eller en aktör som myndigheten anvisat möjlighet att övervaka att kraven på dataskydd och informationssäkerhet uppfylls.	(Jfr 552/2019 30 §)
	Tjänsteleverantören ska bevara uppgifterna om överensstämmelse med kraven och övriga uppgifter som tillsynen kräver i minst fem år efter det att den informationssäkra driftmiljön inte längre används för produktion. Logguppgifterna om användning och utlämnande ska förstöras eller arkiveras tolv år efter det att dataanvändningstillståndet upphört att gälla.	(Jfr 552/2019 29 §, 19 §)
Uppföljning och utvärdering av användningen av en informationssäker driftmiljö	Tjänsteleverantören ska genom ett uppdaterat och systematiskt förfarande följa upp och utvärdera erfarenheterna av en informationssäker driftmiljö under den tid den används för produktion. Tjänsteleverantören ska ge akt på ändringar i lagen och justera driftmiljön i enlighet med ändringarna.	(Jfr 552/2019 29 §)



Tillståndsmyndigheten för användning  
av social- och hälsovårdsdata

Krav på informationssäkra driftmiljöer

Processfas	Uppgifter	Observera
Rådgivning	Tjänsteleverantören erbjuder en tjänstebeskrivning av, en prislista för och rådgivning om den informationssäkra driftmiljön.	Tillståndsmyndigheten tillhandahåller rådgivningstjänster endast om den informationssäkra driftmiljö som myndigheten själv ordnar.
Beställning av en användarmiljö	Kunden gör beställningen genom det förfarande som tjänsteleverantören ordnar i den användarmiljö som nämns i dataanvändningstillståndet och bifogar det officiella beslutet om dataanvändningstillstånd jämte nödvändiga bilagor till beställningen.	Tjänsteleverantören erbjuder kunden möjlighet att uträtta ärenden elektroniskt. Viktiga uppgifter som begärs av kunden utöver de uppgifter som anges i tillståndet är till exempel <ul style="list-style-type: none"> <li>• identifierare för forskningsgruppens medlemmar (identifierande elektroniska identifierare och identitetsfederationer)</li> <li>• kontaktuppgifter till forskningsgruppens medlemmar</li> <li>• kapacitet som användarmiljön behöver</li> <li>• programvara som behövs</li> <li>• faktureringsuppgifter</li> </ul>
	Tjänsteleverantören kontrollerar att ett elektroniskt signerat dataanvändningstillstånd är äkta.	Dataanvändningstillståndet har skickats till kunden elektroniskt undertecknat i pdf-format.
	Tjänsteleverantören bekräftar att beställningen har tagits emot.	–
	Tjänsteleverantören behandlar beställningen.	Beställningen ska basera sig på ett gällande dataanvändningstillstånd och en informationssäker driftmiljö ska ha påvisats i tillståndet. Tjänsteleverantören ber vid behov kunden om mer information om beställningen.
	Tjänsteleverantören bekräftar att beställningen behandlats.	–
Skapande av användarmiljön	Tjänsteleverantören skapar på basis av kundens beställning en användarmiljö för ett specifikt dataanvändningstillstånd.	–

Tillståndsmyndigheten för användning  
av social- och hälsovårdsdata

Krav på informationssäkra driftmiljöer

Processfas	Uppgifter	Observera
	Tjänsteleverantören skapar användarkonton och åtkomsträttigheter för de användare som nämns i tillståndet.	Åtkomsträttigheter kan endast beviljas de användare som nämns i tillståndet för den tid tillståndet är i kraft. Leverantören av en driftmiljö ska innan en anslutning till tillståndshavaren öppnas säkerställa att tillståndshavaren uppfyller kraven i dataanvändningstillståndet. (Jfr 552/2019 51 §) Tjänsteleverantören ska föra register över användarna i den informationssäkra driftmiljön och deras åtkomsträttigheter. Uppgifter om åtkomsträttigheter för användarna i driftmiljön ska förstöras eller arkiveras tolv år efter det att åtkomsträtten upphört att gälla.
Identifiering av användare	Vid identifiering av användare iakttas kraven i denna föreskrift.	(Jfr 552/2019 21 §) Användarna i en informationssäker driftmiljö ska identifieras på ett tillförlitligt sätt och verifieras. Tillförlitlig identifiering kan ske t.ex. via tjänsten Suomi.fi eller en betrodd federerad autentiseringskälla.
Leverans av inloggningsuppgifter till användarna	Tjänsteleverantören ger de personer som nämns i uppgiftstillståndet anvisningar för registrering och inloggning samt anvisningar för aktivering av tvåfaktorsautentisering.	Eventuella uppgifter i anslutning till identifieringskoderna skickas till användaren på ett informationssäkert sätt.
Specifikation av åtkomsträttigheter	De personer som nämns i dataanvändningstillståndet beviljas åtkomsträttigheter till det material som tillståndet gäller. Tjänsteleverantören fastställer åtkomsträttigheterna till personuppgifterna för tillståndshavaren och andra personer som behandlar personuppgifter i driftmiljön.	Alla användare av driftmiljön ska nämnas i det dataanvändningstillstånd som beviljats av Tillståndsmyndigheten. Åtkomsträttigheterna får vara i kraft endast under tillståndets giltighetstid. Tjänsteleverantören ska föra register över användarna i den informationssäkra driftmiljön och deras åtkomsträttigheter. Uppgifter om åtkomsträttigheter för användarna i driftmiljön ska förstöras eller arkiveras tolv år efter det att åtkomsträtten upphört att gälla.
Leverans av material till en informationssäker driftmiljö	Materialet överförs i regel till tjänsteleverantören via en informationssäker drifttjänst.	Om den personuppgiftsansvarige behöver överföra tillståndspliktigt material i sin egen miljö till en egen informationssäker driftmiljö inom samma fysiskt och tekniskt skyddade område, kan överföringen också utföras utan en informationssäker

Tillståndsmyndigheten för användning  
av social- och hälsovårdsdata

Krav på informationssäkra driftmiljöer

Processfas	Uppgifter	Observera
		drifttjänst.
	Tjänsteleverantören säkerställer det mottagna materialets integritet, informationssäkerhet och att det är felfritt.	–
	Tjänsteleverantören gör materialet tillgängligt i användarmiljön för de användare som nämns i tillståndet.	–
Överföring av färdiga produkter från en informationssäker driftmiljö	Tjänsteleverantören överför kundens färdiga produkter via en informationssäker drifttjänst till Tillståndsmyndigheten för granskning i fråga om anonymisering.	Tillståndsmyndigheten kan dock av grundad anledning i sitt tillståndsbeslut ge tillståndshavaren rätt att genomföra anonymiseringen av de ovan nämnda uppgifter som den själv publicerar på villkor att de i efterhand levereras till Tillståndsmyndigheten.
Hantering och genomförande av ändringsbeställningar	Tjänsteleverantören tar emot begäran om ändring och tilläggsbeställningar i anslutning till användarmiljön enligt leverantörens egen tjänstebeskrivning och genomför dem dokumenterat inom ramen för dataanvändningstillståndet.	Ändringarna som kunden beställt får inte genomföras om de strider mot lag eller gällande dataanvändningstillstånd.
Nedstängning av användarmiljön	Tjänsteleverantören nekar åtkomst till användarmiljön efter att dataanvändningstillståndet eller avtalet upphört att gälla, på kundens begäran eller om myndigheten bestämmer det.	–
	Tjänsteleverantören avlägsnar personuppgiftsmaterialet på ett informationssäkert sätt vid en tidpunkt som leverantören och kunden tillsammans kommer överens om, dock senast sex månader efter att dataanvändningstillståndet har upphört, om inte något annat har bestämts.	–